

Application Serial No.: 09/853,164

1

CLAIMS

2 Having thus described our invention, what we claim as new and desire to secure by Letters Patent  
3 is as follows:

4 1. (original) A method comprising:

5 enabling at least one client to access restricted information from an origin web-server through a  
6 semi-trusted web-server including the steps of:

7 authenticating said at least one client;

8 creating a client credential having client-specific environment information for each said at least  
9 one client;

10 presenting the client credential to the semi-trusted web-server;

11 correlating said at least one client with the client credential; and

12 providing said access to said at least one client.

13 2. (original) A method as recited in claim 1, further comprising serving the restricted information  
14 to said at least one client through the semi-trusted web-server.

15 3. (original) A method as in claim 1, wherein the step of creating comprises storing the  
16 client-specific environment information and the client credential in a cookie in said at least one  
17 client's browser.

Docket No.: YOR920010426US1

-2-

Application Serial No.: 09/853,164

- 1    4. (original) A method as in claim 1, wherein the step of presenting comprises:
  - 2    sending the client credential to the semi-trusted web-server; and
  - 3    using HTTP redirection to refer said at least one client to the semi-trusted web-server. (original)
- 4    5. (original) A method as in claim 1, wherein the step of presenting comprises:
  - 5    sending said at least one client credential to a directory accessible to the semi-trusted web-server;
  - 6    and
- 7    the origin web-server using HTTP redirection to send said at least one client to the semi-trusted web-server.
- 9    6. (original) A method as in claim 1, wherein the step of creating comprises:
  - 10    collecting the client-specific environment information; and
  - 11    storing the client-specific environment information in the client credential.
- 12    7. (original) A method as in claim 6, wherein the client-specific environment information includes:
  - 14    a hash of the HTTP-Request header of said at least one client request;
  - 15    a hash of the IP address of the machine used by said at least one client;
  - 16    a process identity of said at least one client browser;

Docket No.: YOR920010426US1

-3-

Application Serial No.: 09/853,164

- 1 a hash of a user identity used by said at least one client program; and/or
- 2 any combination of these.
- 3 8. (original) A method as in claim 1, wherein the step of creating comprises:
  - 4 placing a first client-side program at said at least one client;
  - 5 collecting a first set of the client-specific environment information using the first client-side program;
  - 6 sending the first set of the client-specific environment information to the origin web-server; and
  - 7 storing the first set of the client-specific environment information in the client credential.
- 9 9. (original) A method as in claim 8, wherein the step of correlating includes:
  - 10 the semi-trusted web-server placing a second client-side program at said at least one client;
  - 11 collecting a second set of the client-specific environment information with the second client-side program;
  - 13 sending the second set of the client-specific environment information to the semi-trusted web-server; and
  - 15 correlating the second set of the client-specific environment information to the client credential.
- 16 10. (original) A method as in claim 9, wherein the first and/or the second client-specific environment information includes: a hash of the HTTP-Request header of said at least one client request; a hash of the IP address of the machine used by said at least one client; a process identity

Docket No.: YOR920010426US1

-4-

Application Serial No.: 09/853,164

1 of said at least one client browser; a hash of a user identity used by said at least one client  
2 program; and/or any combination of these.

3 11. (original) A method as in claim 1, further comprising the semi-trusted web-server accessing  
4 an encrypted version of the restricted information, and wherein the step of creating the client  
5 credential includes adding a decryption key to the client credential.

6 12. (original) A method as in claim 11 wherein the decryption key is a partial key, and the step of  
7 providing includes the semi-trusted web-server supplying information to said at least one client  
8 enabling conversion of the partial key to a full key.

9 13. (original) A method as in claim 1 wherein the step of authenticating includes employing a  
10 user-password scheme.

11 14. (original) A method as in claim 1, wherein the step of authenticating includes deploying at  
12 least one certificate.

13 15. (original) A method as in claim 6, wherein the step of collecting the client-specific  
14 environment information is performed by the origin web-server, and

15 the origin web-server storing the client-specific environment information in the client credential.

16 16. (original) A method as in claim 8, wherein the steps of placing and the step of storing is  
17 performed by the origin web-server.

18 17. (original) A method as recited in claim 1, wherein the semi-trusted web-server is a proxy  
19 web-server.

20 18. (original) A method as recited in claim 1, wherein the step of creating a credential for said at  
21 least one client at an origin web-server;

Docket No.: **YOR920010426US1**

-5-

Application Serial No.: 09/853,164

- 1        19. (original) A method as recited in claim 1, wherein the step of correlating said at least one
- 2        client and the client credential is performed by the semi-trusted web-server.
  
- 3        20. (original) A method as recited in claim 1, wherein the step of authenticating said at least one
- 4        client is performed at the origin web-server.
  
- 5        21. (currently amended) An apparatus for enabling at least one client to access restricted
- 6        information from an origin web-server through a semi-trusted web-server, said apparatus
- 7        comprising:
  - 8            an authenticator to validate said at least one client;
  
  - 9            a credential creator to create a client credential having client-specific environment information
  - 10          for each said at least one client; and
  
  - 11          a correlator for matching said at least one client to the client credential, and for working in
  - 12          combination with said authenticator and said credential creator to enable said at least one client
  - 13          to safely access restricted information from the origin web-server through the semi-trusted
  - 14          web-server.
  
- 15        22. (original) The apparatus as in claim 21, wherein the credential creator stores the
- 16        client-specific environment information in a cookie set in said at least one client's browser.
  
- 17        23. (original) An apparatus as in claim 21, wherein the credential creator presents the credential
- 18        to the semi-trusted web-server.
  
- 19        24. (original) The apparatus as in claim 21, wherein the credential creator stores a client-side
- 20        program in said at least one client's browser.

Docket No.: YOR920010426US1

-6-

Application Serial No.: 09/853,164

- 1    25. (original) The apparatus as in claim 21, wherein the correlator stores a second client-side
- 2    program in the client's browser.
  
- 3    26. (original) The apparatus as in claim 21, wherein the semi-trusted web-server has access only
- 4    to an encrypted version of the restricted information, and the credential creator adds a decryption
- 5    key to the client credential.
  
- 6    27. (original) The apparatus as in claim 26, wherein the decryption key is a partial key and the
- 7    semi-trusted web-server includes an information supplier to supply said at least one client with
- 8    information to enable conversion of the partial key to a full key.
  
- 9    28. (original) An article of manufacture comprising a computer usable medium having computer
- 10   readable program code means embodied therein for enabling at least one client to access
- 11   restricted information from an origin web-server through a semi-trusted web-server, the
- 12   computer readable program code means in said article of manufacture comprising computer
- 13   readable program code means for causing a computer to effect the steps of claim 1.
  
- 14   29: An article of manufacture as recited in claim 28, the computer readable program code means
- 15   in said article of manufacture further comprising computer readable program code means for
- 16   causing a computer to effect the steps of claim 12.
  
- 17   30. (original) A program storage device readable by machine, tangibly embodying a program of
- 18   instructions executable by the machine to perform method steps for enabling at least one client to
- 19   access restricted information from an origin web-server through a semi-trusted web-server, said
- 20   method steps comprising the steps of claim 1.
  
- 21   31. (original) An apparatus comprising:
  
- 22   means for enabling at least one client to access restricted information from an origin web-server
- 23   through a semi-trusted web-server including:

Docket No.: YOR920010426US1

-7-

Application Serial No.: 09/853,164

- 1 means for authenticating said at least one client;
- 2 means for creating a client credential having client-specific environment information for each  
3 said at least one client;
- 4 means for presenting the client credential to the semi-trusted web-server;
- 5 means for correlating said at least one client with the client credential; and
- 6 means for providing said access to said at least one client.

7 32. (original) An apparatus as recited in claim 31, further comprising means for serving the  
8 restricted information to said at least one client through the semi-trusted web-server.

9 33. (original) An apparatus as in claim 31, further comprising means for storing the  
10 client-specific environment information and the client credential in a cookie in said at least one  
11 client's browser.

12 34. (original) An apparatus as in claim 31, further comprising means for:  
13 sending the client credential to the semi-trusted web-server; and  
14 using HTTP redirection to refer said at least one client to the semi-trusted web-server. (original)

15 35. (original) An apparatus as in claim 31, wherein the origin web-server uses HTTP redirection  
16 to send said at least one client to the semi-trusted web-server, and further comprising means for  
17 sending said at least one client credential to a directory accessible to the semi-trusted web-server.

18 36. (original) An apparatus as in claim 31, further comprising means for:

Docket No.: YOR920010426US1

-8-

Application Serial No.: 09/853,164

- 1 collecting the client-specific environment information; and
- 2 storing the client-specific environment information in the client credential.
- 3 37. (original) An apparatus as in claim 36, wherein the client-specific environment information includes:
  - 5 a hash of the HTTP-Request header of said at least one client request;
  - 6 a hash of the IP address of the machine used by said at least one client;
  - 7 a process identity of said at least one client browser;
  - 8 a hash of a user identity used by said at least one client program; and/or
  - 9 any combination of these.
- 10 38. (original) An apparatus as in claim 31, further comprising means for:
  - 11 placing a first client-side program at said at least one client;
  - 12 collecting a first set of the client-specific environment information using the first client-side program;
  - 14 sending the first set of the client-specific environment information to the origin web-server; and
  - 15 storing the first set of the client-specific environment information in the client credential.
- 16 39. (original) An apparatus as in claim 38, further comprising means for:

Docket No.: YOR920010426US1

-9-

Application Serial No.: 09/853,164

- 1 the semi-trusted web-server to place a second client-side program at said at least one client;
- 2 collecting a second set of the client-specific environment information with the second client-side
- 3 program;
- 4 sending the second set of the client-specific environment information to the semi-trusted
- 5 web-server; and
- 6 correlating the second set of the client-specific environment information to the client credential.

7 40. (original) An apparatus as in claim 39, wherein the first and/or the second client-specific

8 environment information includes:

- 9 a hash of the HTTP-Request header of said at least one client request;
- 10 a hash of the IP address of the machine used by said at least one client;
- 11 a process identity of said at least one client browser;
- 12 a hash of a user identity used by said at least one client program;
- 13 and/or any combination of these.

14 41. (original) An apparatus as in claim 31, further comprising means for the semi-trusted

15 web-server to access an encrypted version of the restricted information, and means for adding a

16 decryption key to the client credential during creation.

Docket No.: YOR920010426US1

-10-

Application Serial No.: 09/853,164

1    42. (original) An apparatus as in claim 41, wherein the decryption key is a partial key comprising  
2    means for the semi-trusted web-server to supply information to said at least one client enabling  
3    conversion of the partial key to a full key.

4    43. (original) An apparatus as in claim 31, further comprising of a means for authenticating by  
5    employing a user-password scheme.

6    44. (original) An apparatus as in claim 31, further comprising of a means for authenticating by  
7    deploying at least one certificate.

8    45. (original) A computer program product comprising a computer usable medium having  
9    computer readable program code means embodied therein for causing enablement of at least one  
10   client to access restricted information from an origin web-server through a semi-trusted  
11   web-server, the computer readable program code means in said computer program product  
12   comprising computer readable program code means for causing a computer to effect the  
13   apparatus of claim 31.

14   46. (original) A computer program product comprising a computer usable medium having  
15   computer readable program code means embodied therein for causing enablement of at least one  
16   client to access restricted information from an origin web-server through a semi-trusted  
17   web-server, the computer readable program code means in said computer program product  
18   comprising computer readable program code means for causing a computer to effect the  
19   apparatus of claim 21.  
20

Docket No.: YOR920010426US1

-11-

PAGE 11/14 \* RCV'D AT 1/6/2005 2:47:54 PM [Eastern Standard Time] \* SVR:USPTO-EFXRF-1/0 \* DNIS:8729306 \* CSID:9149453281 \* DURATION (mm:ss):04:12